ISFD PKI Enablement

Background:

During the Fall of 2012 Defense Security Service will be integrating ISFD with the Identity Management (IdM) Solution, in compliance with the Joint Task Force-Global Network Operations requirement that "all components allow only certificate-based client authentication to

private Department of Defense (DoD) Web servers using certificates issued by DoD Public Key Infrastructure (PKI) Certificate Authorities." Following the integration effort, ISFD users will no longer be permitted to access ISFD directly from the web, but will be required to authenticate through IdM prior to logging into ISFD.

Impact:

Users will be required to undergo a registration process* of up to three steps. Instructions detailing the ISFD PKI related registration processes are contained within the following pages**.

- IdM Account Registration
- Certificate (CAC/PKI) Registration
- ISFD Account Request (new ISFD users only)

***This process serves as a precursor to Certificate-only access for ISFD, coming in 2013.**

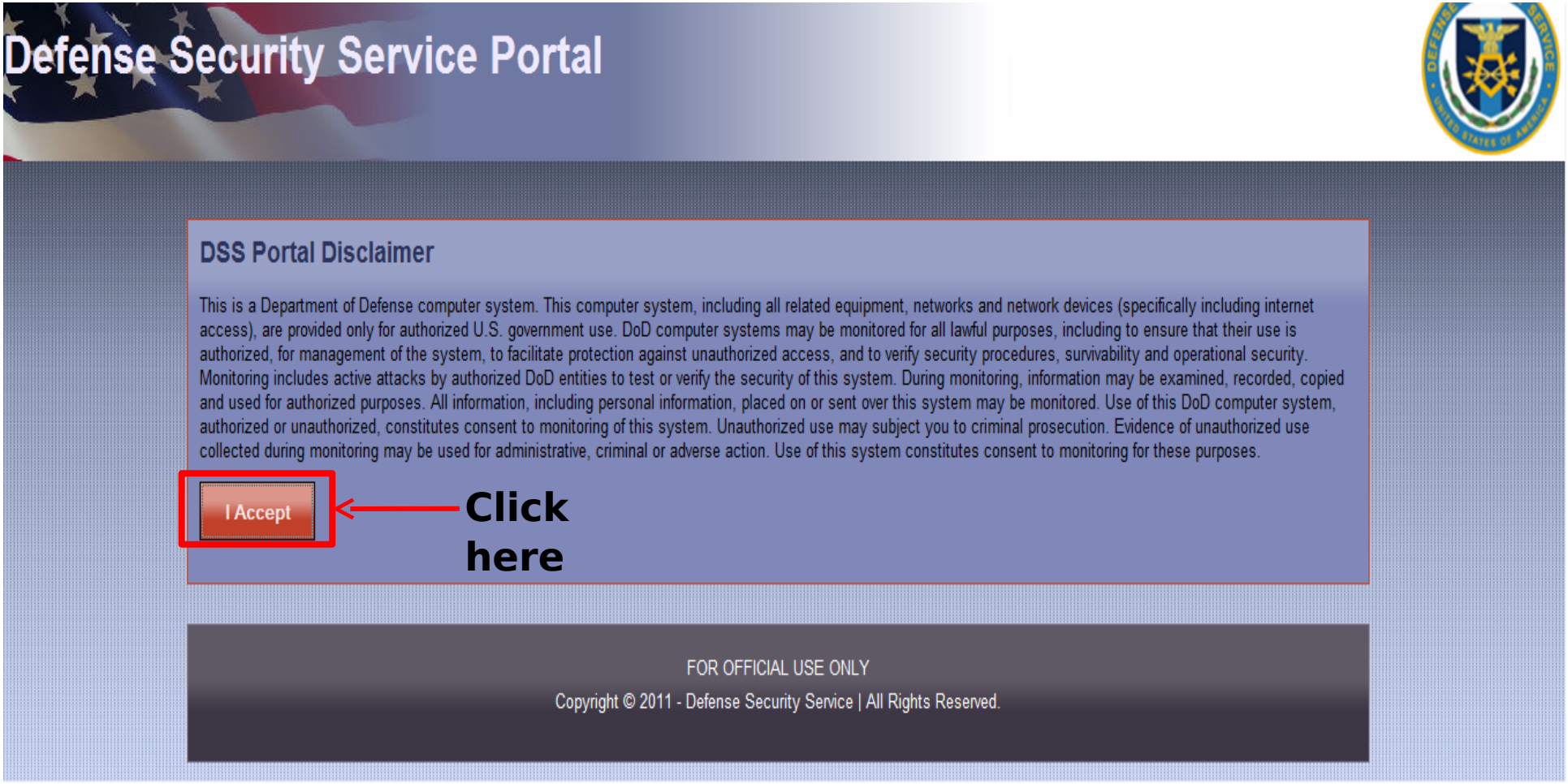
****Final screens and data fields are subject to change.**

IdM Account Registration

Note: There are no approvals required for establishing an IdM Portal account.

IdM Account Registration

Step 1: The User navigates to https://sso.dss.mil.
Step 2: The IdM Solution displays the IdM Portal Disclaimer.
Step 3: The User selects “I Accept” to proceed.


Defense Security Service Portal
DSS Portal Disclaimer
This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including internet access), are provided only for authorized U.S. government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.
I Accept
Click here
FOR OFFICIAL USE ONLY
Copyright © 2011 - Defense Security Service | All Rights Reserved.

IdM Account Registration

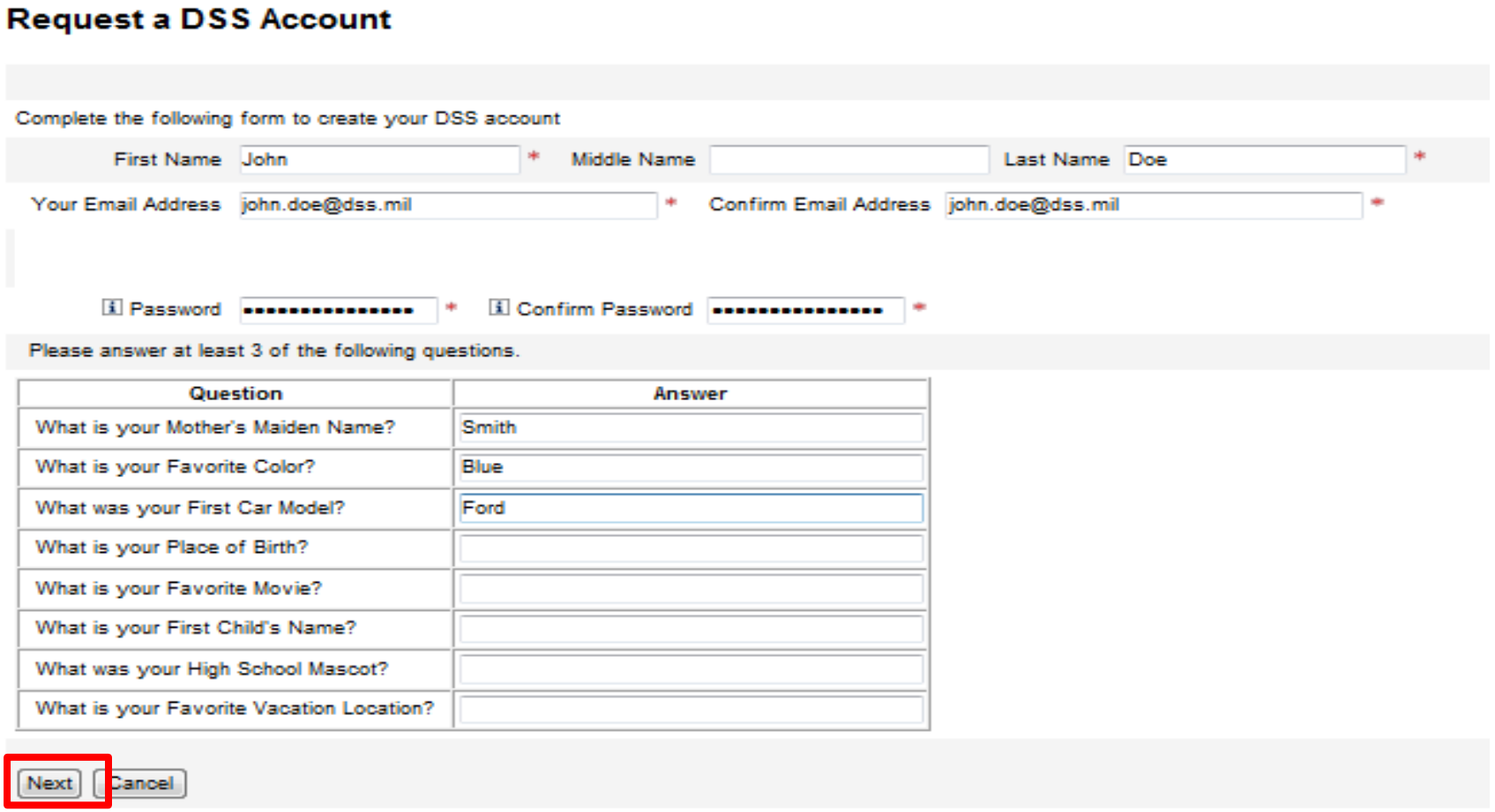
Step 4: The User is shown the unauthenticated IdM Portal page and clicks "Register for an account" to proceed.

Note: If you have recently used your CAC/ECA to login, you may not be prompted for your PIN and/or Certificate.
Login to DSS Portal
CAC/ECA Login
Register CAC/ECA
Register Certificate
Self Enrollment
Register for an account
Threat Advisory
NTAS
NO ACTIVE ALERTS
www.DHS.gov/alerts
Read more
Links
DSS Applications
ODAA
Click here
FAQs
How to Setup Firefox to use ActivClient?
DSS Portal not loading in Firefox?
What is the DSS Portal?
What is the Single Sign-on?
How do I register for a DSS account?
How to reset your password?
How do I associate CAC/ECA with my account?
From where do I get an ECA certificate?
How do I log into DSS Portal using my CAC/ECA?
How can I find help?
CAC error message "Page cannot be displayed"?
See ALL FAQs

IdM Account Registration

Step 5: The User is presented with the IdM Portal account request form, completes all required form fields, and clicks "Next“.

Complete form


Request a DSS Account
Complete the following form to create your DSS account
First Name John * Middle Name Last Name Doe *
Your Email Address john.doe@dss.mil * Confirm Email Address john.doe@dss.mil *
Password ********** * Confirm Password ********** *
Please answer at least 3 of the following questions.
Question
Answer
What is your Mother's Maiden Name?
Smith
What is your Favorite Color?
Blue
What was your First Car Model?
Ford
What is your Place of Birth?
What is your Favorite Movie?
What is your First Child's Name?
What was your High School Mascot?
What is your Favorite Vacation Location?
Next
Cancel

Click Next

IdM Account Registration

Step 6: The User is shown a confirmation screen with the IdM Privacy Act Statement, reviews the user information, reads and accepts the terms of the privacy policy, and clicks "Register".

Step 7: The IdM Solution automatically creates the User's account and notifies the User via email.

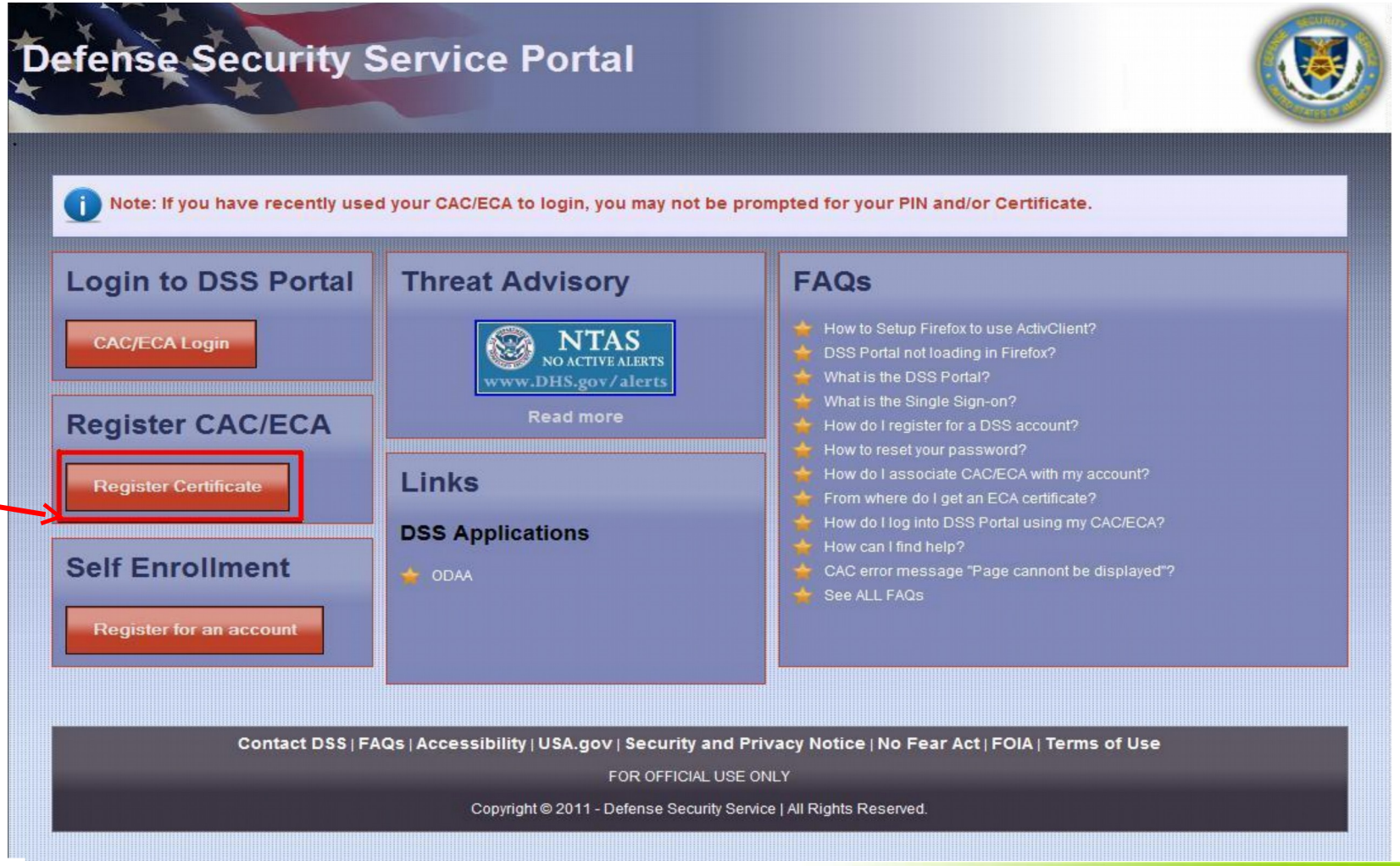
User Information
Account Type
User
First name
John
Middle name
Last name
Doe
E-mail address
john.doe@dss.mil
Privacy Act Statement
Please read and accept this following text
AUTHORITY:
Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PURPOSE:
To record names, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES:
In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: To a Federal, State, or local law enforcement agency when your agency becomes aware of a
I have read and understand the terms of the privacy policy.
Register
Edit
Cancel
Click here to acknowledge the privacy policy
Then click here

Certificate Registration

Certificate Registration

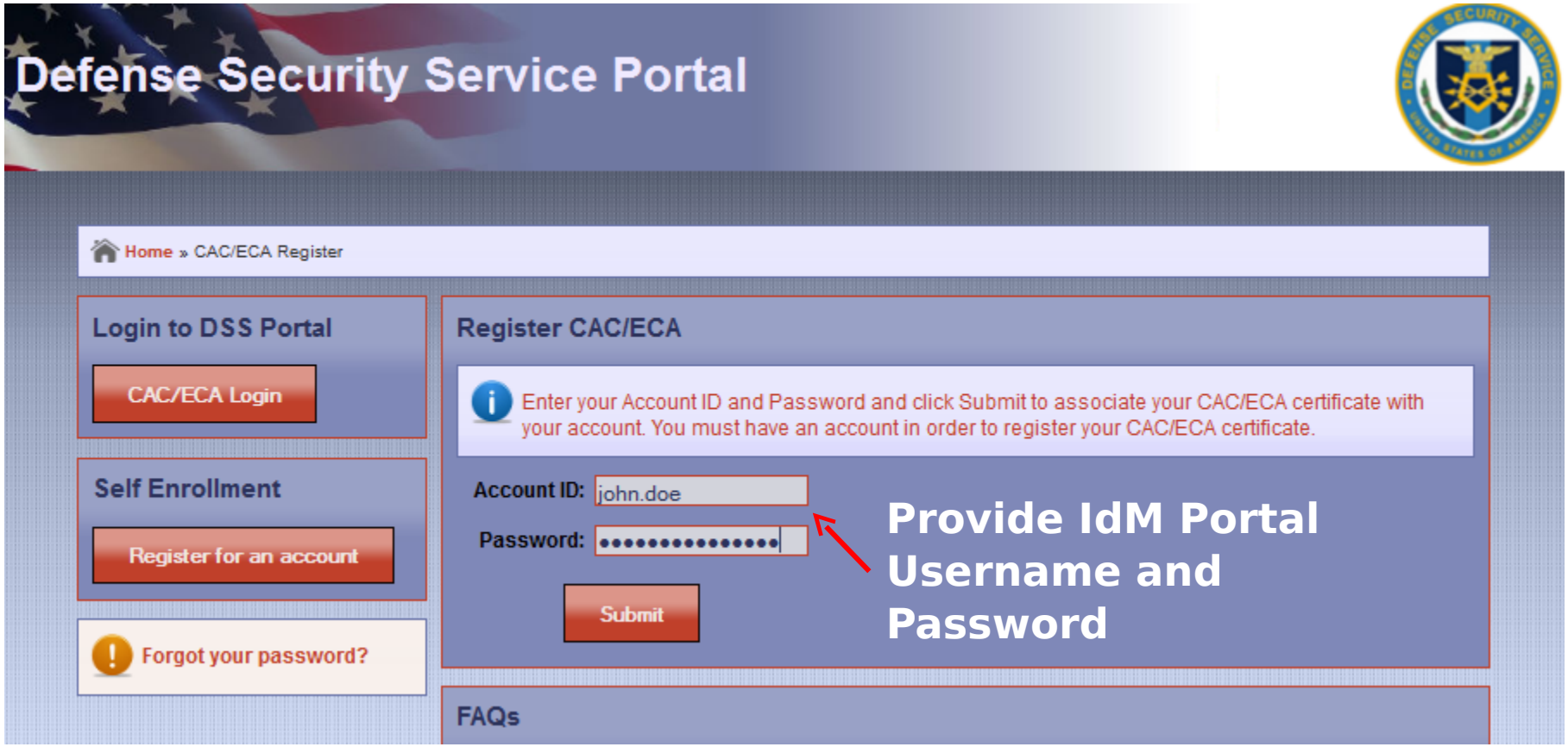
Step 1: The User navigates to https://sso.dss.mil.
Step 2: The IdM Solution displays the IdM Portal Disclaimer.
Step 3 The User selects “I Accept” to proceed.
Step 4: The User is shown the unauthenticated IdM Portal page and clicks “Register Certificate” to proceed.

Click here


Defense Security Service Portal
Note: If you have recently used your CAC/ECA to login, you may not be prompted for your PIN and/or Certificate.
Login to DSS Portal
CAC/ECA Login
Register CAC/ECA
Register Certificate
Self Enrollment
Register for an account
Threat Advisory
NTAS
NO ACTIVE ALERTS
www.DHS.gov/alerts
Read more
Links
DSS Applications
ODAA
FAQs
How to Setup Firefox to use ActivClient?
DSS Portal not loading in Firefox?
What is the DSS Portal?
What is the Single Sign-on?
How do I register for a DSS account?
How to reset your password?
How do I associate CAC/ECA with my account?
From where do I get an ECA certificate?
How do I log into DSS Portal using my CAC/ECA?
How can I find help?
CAC error message "Page cannont be displayed"?
See ALL FAQs
Contact DSS | FAQs | Accessibility | USA.gov | Security and Privacy Notice | No Fear Act | FOIA | Terms of Use
FOR OFFICIAL USE ONLY
Copyright © 2011 - Defense Security Service | All Rights Reserved.

Certificate Registration

Step 5: The User enters their IdM Portal Account ID (supplied in the account creation email) and the password that he/she set during the self-enrollment process.
Step 6: The User clicks “Submit”.


Defense Security Service Portal
Home » CAC/ECA Register
Login to DSS Portal
CAC/ECA Login
Self Enrollment
Register for an account
Forgot your password?
Register CAC/ECA
Enter your Account ID and Password and click Submit to associate your CAC/ECA certificate with your account. You must have an account in order to register your CAC/ECA certificate.
Account ID: john.doe
Password:
Submit
Provide IdM Portal Username and Password
FAQs

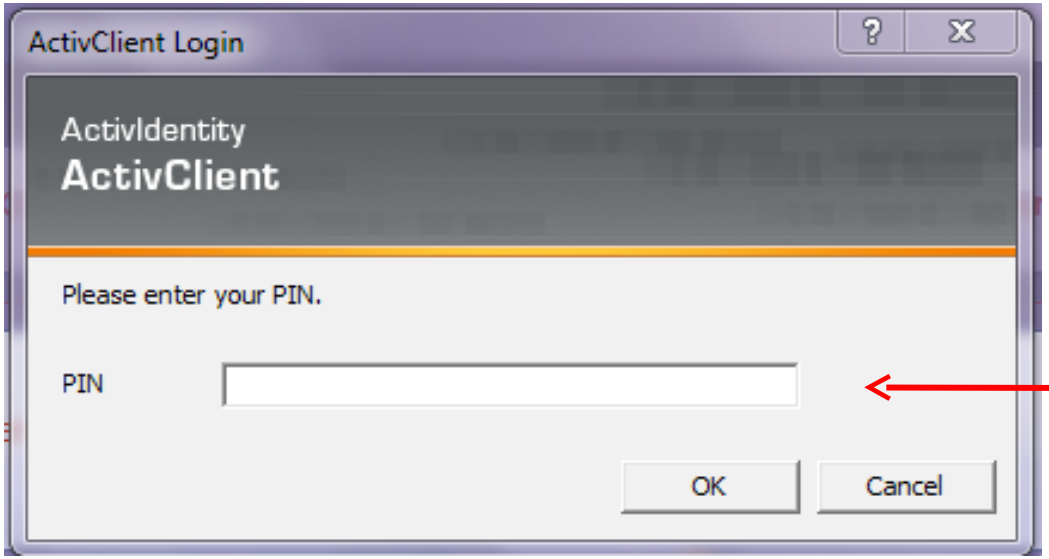
Certificate Registration

Step 7: Upon clicking submit, a pop-up box containing a list of digital certificates will appear; User selects the appropriate DoD CAC/External Certificate Authority (ECA), non-email, user specific certificate.

Select appropriate certificate

Certificate Registration

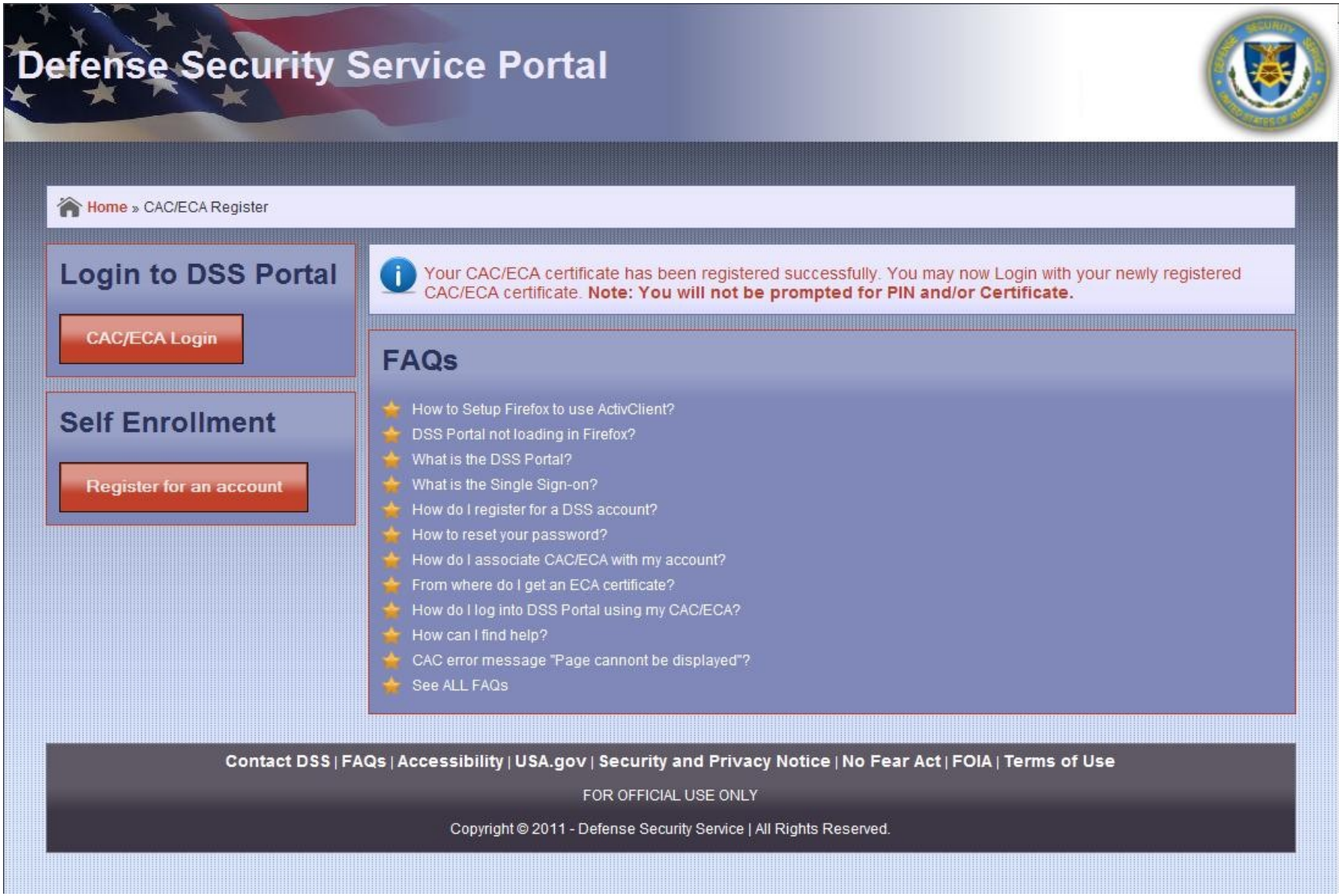
Step 8: The User enters his/her PIN.



Enter PIN

Certificate Registration

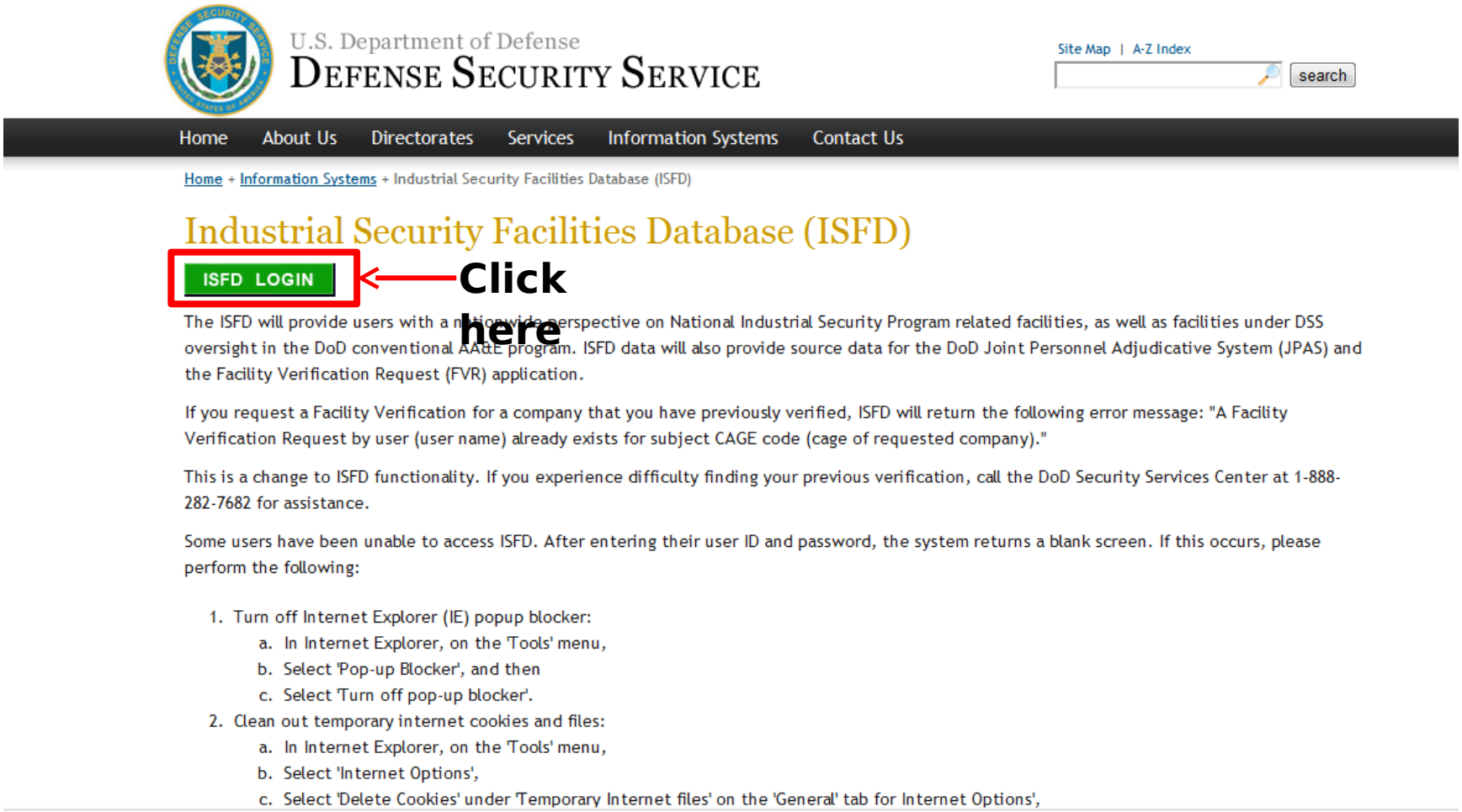
Step 9: If successful, a confirmation message will be displayed informing the User that their certificate was registered successfully, and the User enters the IdM Portal.


Defense Security Service Portal
Home » CAC/ECA Register
Login to DSS Portal
CAC/ECA Login
Self Enrollment
Register for an account
Your CAC/ECA certificate has been registered successfully. You may now Login with your newly registered CAC/ECA certificate. Note: You will not be prompted for PIN and/or Certificate.
FAQs
How to Setup Firefox to use ActivClient?
DSS Portal not loading in Firefox?
What is the DSS Portal?
What is the Single Sign-on?
How do I register for a DSS account?
How to reset your password?
How do I associate CAC/ECA with my account?
From where do I get an ECA certificate?
How do I log into DSS Portal using my CAC/ECA?
How can I find help?
CAC error message "Page cannont be displayed"?
See ALL FAQs
Contact DSS | FAQs | Accessibility | USA.gov | Security and Privacy Notice | No Fear Act | FOIA | Terms of Use
FOR OFFICIAL USE ONLY
Copyright © 2011 - Defense Security Service | All Rights Reserved.

CAC/PKI Authentication from ISFD Homepage

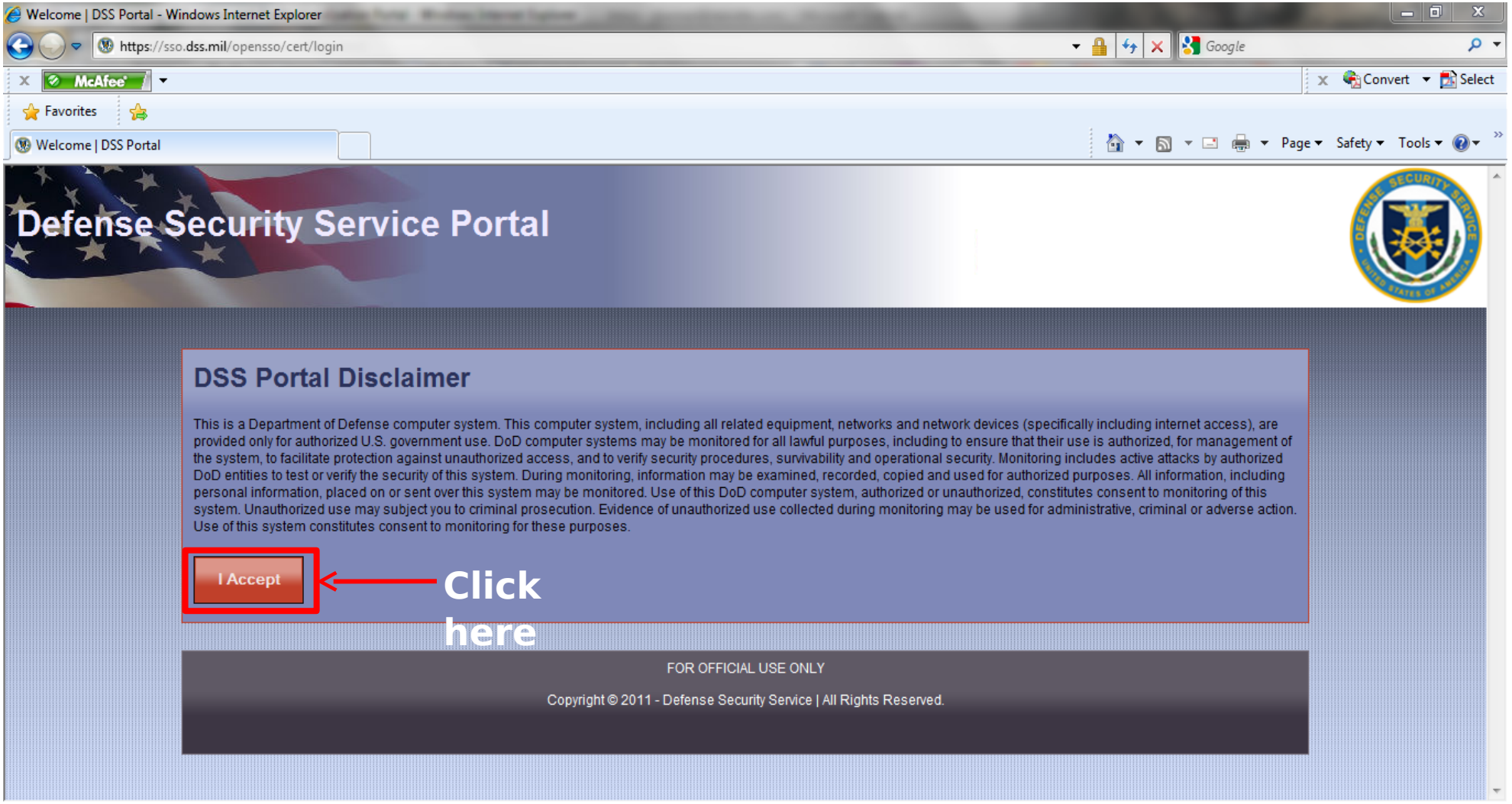
CAC/PKI Authentication from ISFD Homepage

Step 1: Select “ISFD Login” from the unauthenticated ISFD page.


U.S. Department of Defense
DEFENSE SECURITY SERVICE
Site Map | A-Z Index
search
Home
About Us
Directorates
Services
Information Systems
Contact Us
Home + Information Systems + Industrial Security Facilities Database (ISFD)
Industrial Security Facilities Database (ISFD)
ISFD LOGIN
Click here
The ISFD will provide users with a nationwide perspective on National Industrial Security Program related facilities, as well as facilities under DSS oversight in the DoD conventional AA&E program. ISFD data will also provide source data for the DoD Joint Personnel Adjudicative System (JPAS) and the Facility Verification Request (FVR) application.
If you request a Facility Verification for a company that you have previously verified, ISFD will return the following error message: "A Facility Verification Request by user (user name) already exists for subject CAGE code (cage of requested company)."
This is a change to ISFD functionality. If you experience difficulty finding your previous verification, call the DoD Security Services Center at 1-888-282-7682 for assistance.
Some users have been unable to access ISFD. After entering their user ID and password, the system returns a blank screen. If this occurs, please perform the following:
1. Turn off Internet Explorer (IE) popup blocker:
a. In Internet Explorer, on the 'Tools' menu,
b. Select 'Pop-up Blocker', and then
c. Select 'Turn off pop-up blocker'.
2. Clean out temporary internet cookies and files:
a. In Internet Explorer, on the 'Tools' menu,
b. Select 'Internet Options',
c. Select 'Delete Cookies' under 'Temporary Internet files' on the 'General' tab for Internet Options',

CAC/PKI Authentication from ISFD Homepage

Step 2: The IdM solution displays the IdM Portal Disclaimer.
Step 3: User selects "I Accept" to proceed.


Welcome | DSS Portal - Windows Internet Explorer
https://sso.dss.mil/opensso/cert/login
Google
McAfee
Convert
Select
Favorites
Welcome | DSS Portal
Page
Safety
Tools
Defense Security Service Portal
DSS Portal Disclaimer
This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including internet access), are provided only for authorized U.S. government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.
I Accept
Click here
FOR OFFICIAL USE ONLY
Copyright © 2011 - Defense Security Service | All Rights Reserved.

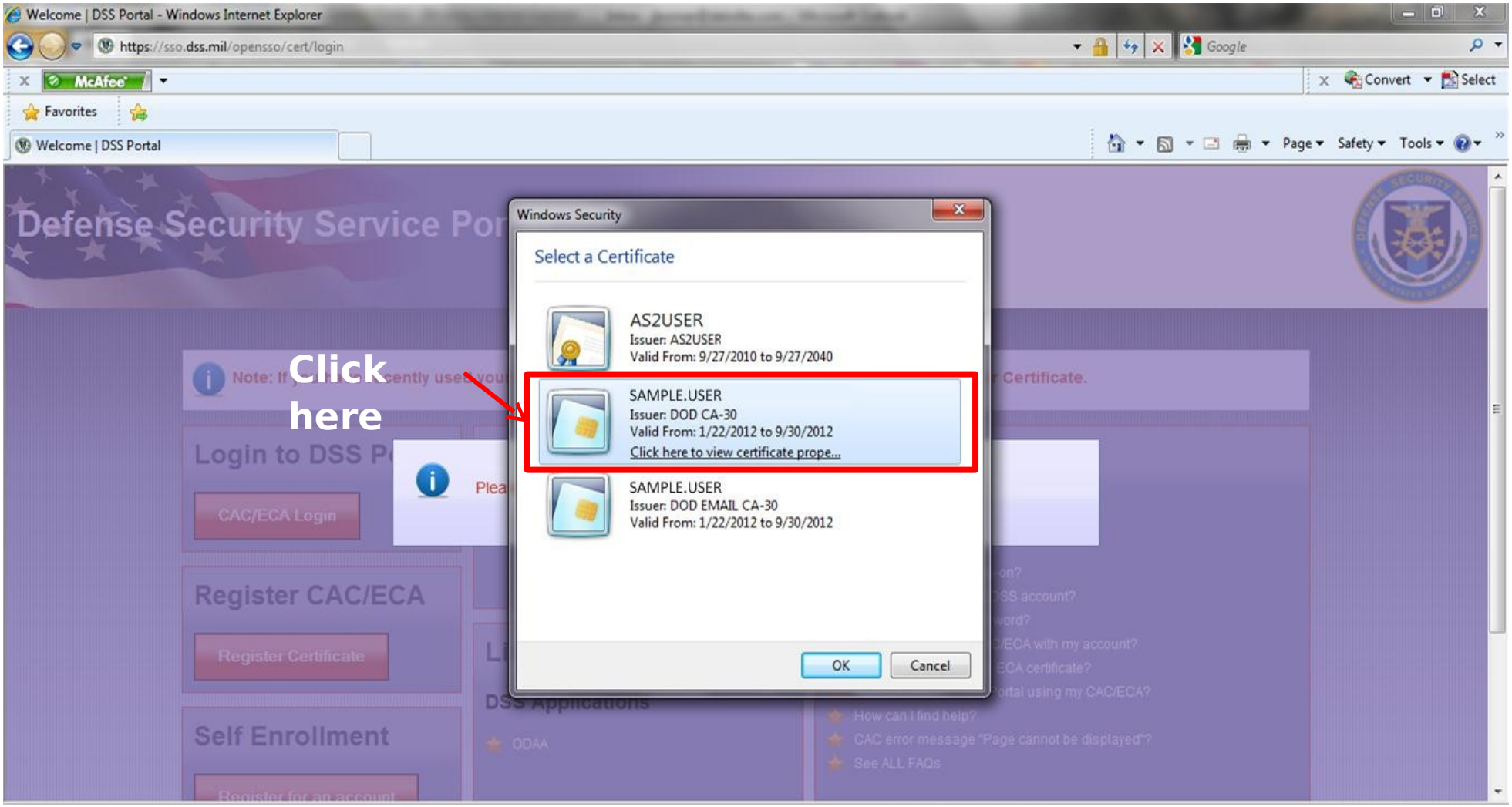
CAC/PKI Authentication from ISFD Homepage

Step 4: The IdM solution displays the unauthenticated IdM homepage.
Step 5: User selects “CAC/ECA Login”.

Defense Security Service Portal
Welcome ISFD user
Note: If you have recently used your CAC/ECA to login, you may not be prompted for your PIN and/or Certificate.
Login to DSS Portal
CAC/ECA Login
Register CAC/ECA
Register Certificate
Self Enrollment
Register for an account
Threat Advisory
NTAS
NO ACTIVE ALERTS
www.DHS.gov/alerts
Read more
Links
DSS Applications
STEPP
OBMS
ISFD
Click here
FAQs
How to Setup Firefox to use ActivClient?
DSS Portal not loading in Firefox?
What is the DSS Portal?
What is the Single Sign-on?
How do I register for a DSS account?
How to reset your password?
How do I associate CAC/ECA with my account?
From where do I get an ECA certificate?
How do I log into DSS Portal using my CAC/ECA?
How can I find help?
CAC error message "Page cannot be displayed"?
See ALL FAQs
Contact DSS | FAQs | Accessibility | USA.gov | Security and Privacy Notice | No Fear Act | FOIA | Terms of Use
FOR OFFICIAL USE ONLY
Copyright © 2011 - Defense Security Service | All Rights Reserved.

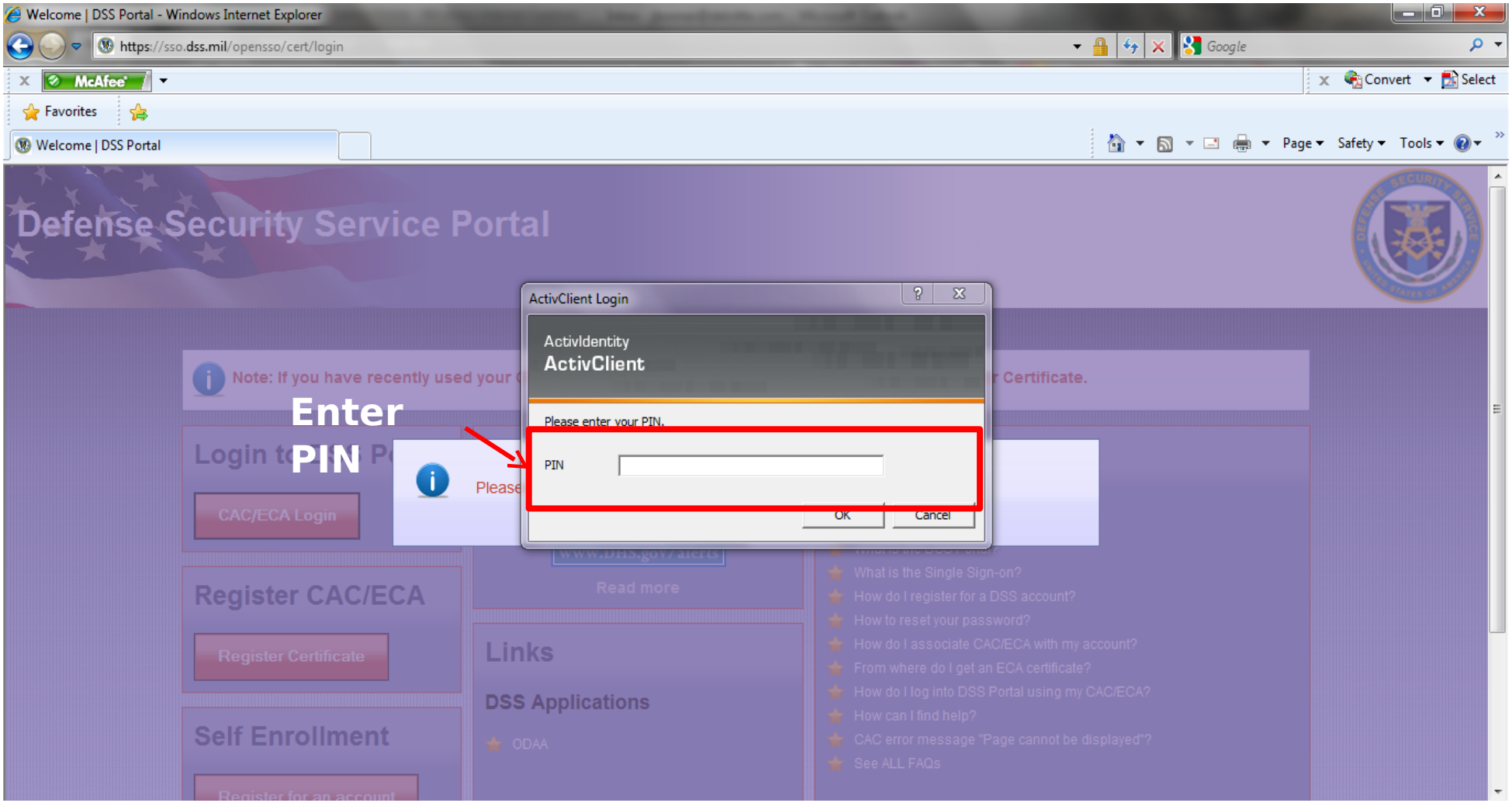
CAC/PKI Authentication from ISFD Homepage

Step 6: User selects appropriate certificate.



CAC/PKI Authentication from ISFD Homepage

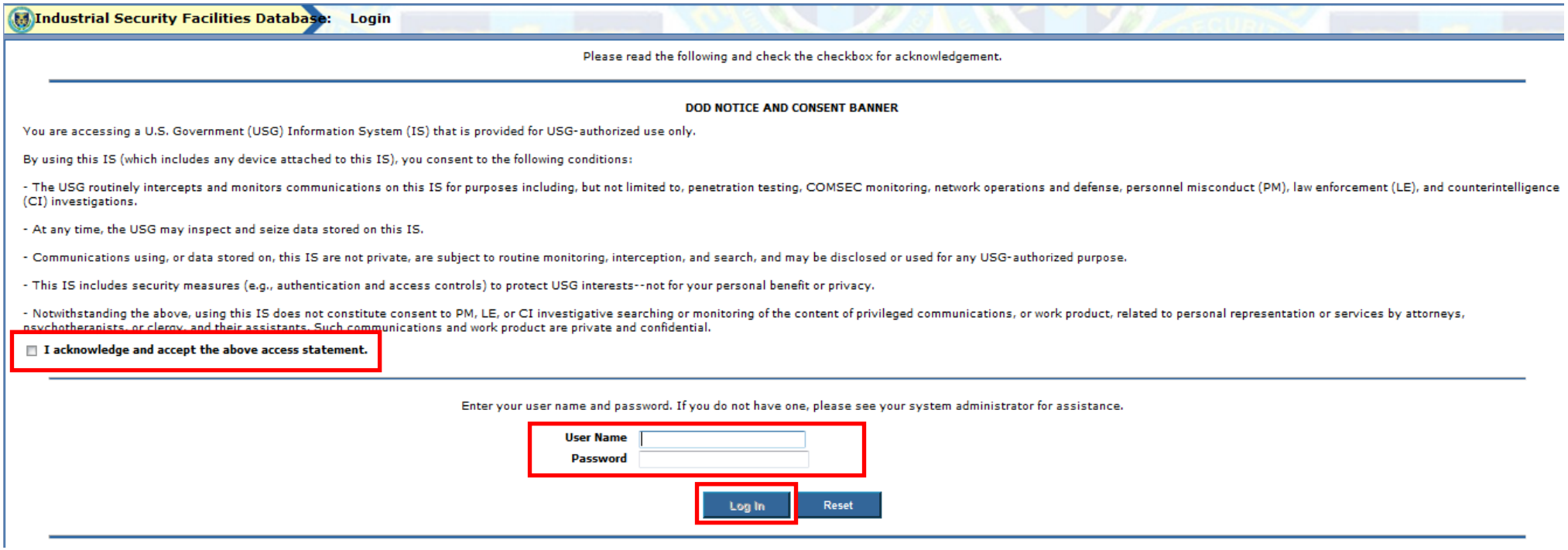
Step 7: User enters PIN when prompted.



CAC/PKI Authentication from ISFD Homepage

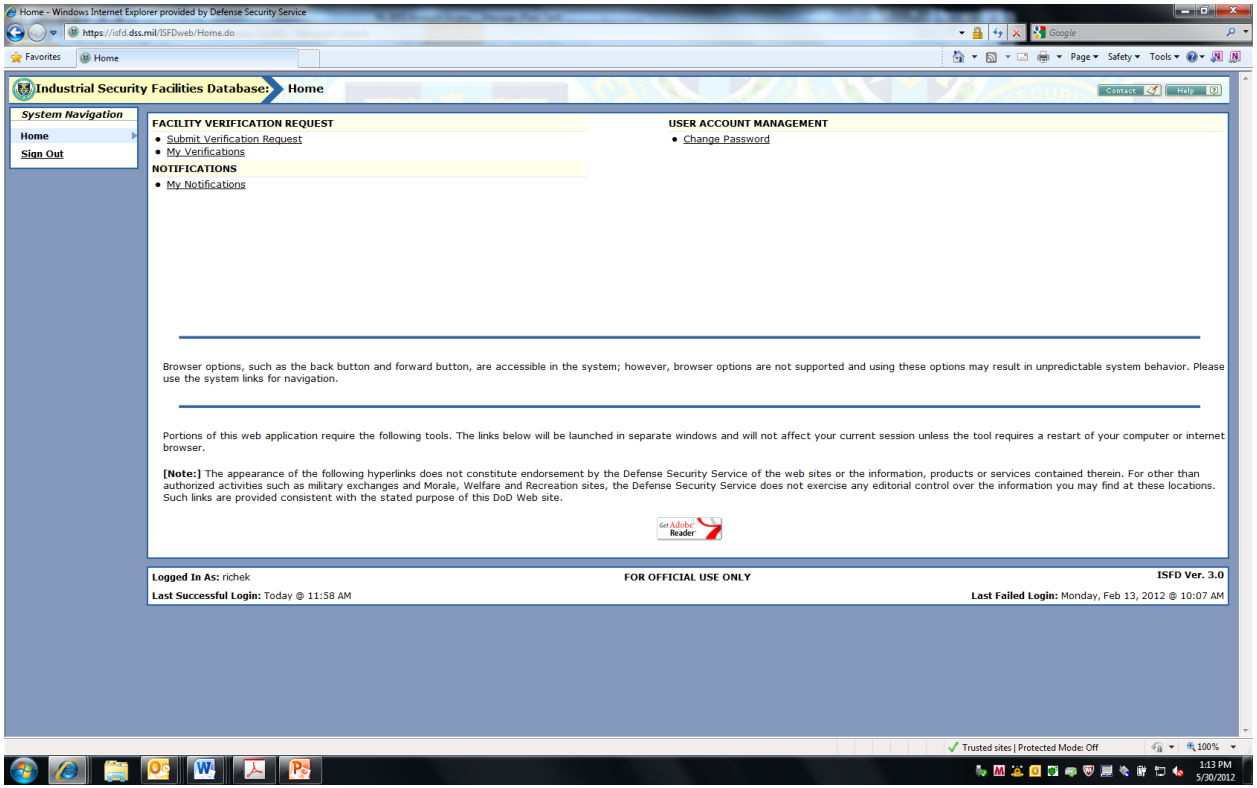
Step 8: The IdM solution authenticates the User and redirects him/her to the ISFD Username/Password Login page.

Step 9: User agrees to the disclaimer, enters his/her ISFD Username and Password, and clicks “Log In”.


Industrial Security Facilities Database: Login
Please read the following and check the checkbox for acknowledgement.
DOD NOTICE AND CONSENT BANNER
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential.
I acknowledge and accept the above access statement.
Enter your user name and password. If you do not have one, please see your system administrator for assistance.
User Name
Password
Log In
Reset

CAC/PKI Authentication from ISFD Homepage

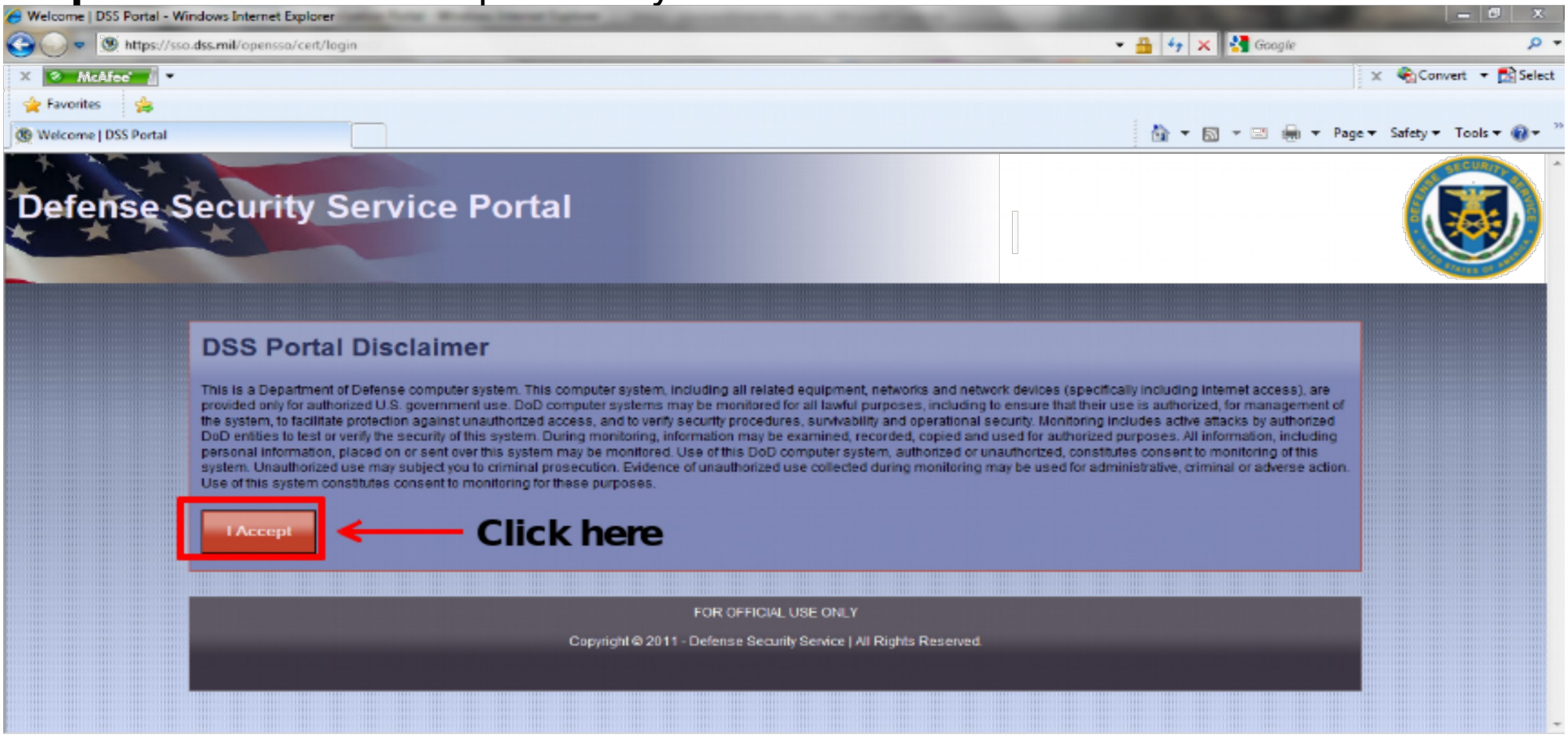
Step 10: ISFD authenticates the User and allows full access.


Home - Windows Internet Explorer provided by Defense Security Service
https://isfd.dss.mil/ISFDweb/Home.do
Favorites
Home
Industrial Security Facilities Database:
Home
Contact
Help
System Navigation
Home
Sign Out
FACILITY VERIFICATION REQUEST
Submit Verification Request
My Verifications
NOTIFICATIONS
My Notifications
USER ACCOUNT MANAGEMENT
Change Password
Browser options, such as the back button and forward button, are accessible in the system; however, browser options are not supported and using these options may result in unpredictable system behavior. Please use the system links for navigation.
Portions of this web application require the following tools. The links below will be launched in separate windows and will not affect your current session unless the tool requires a restart of your computer or internet browser.
[Note:] The appearance of the following hyperlinks does not constitute endorsement by the Defense Security Service of the web sites or the information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare and Recreation sites, the Defense Security Service does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this DoD Web site.
Get Adobe Reader
Logged In As: richek
FOR OFFICIAL USE ONLY
ISFD Ver. 3.0
Last Successful Login: Today @ 11:58 AM
Last Failed Login: Monday, Feb 13, 2012 @ 10:07 AM
Trusted sites | Protected Mode: Off
100%
1:13 PM
5/30/2012

ISFD Access from IdM

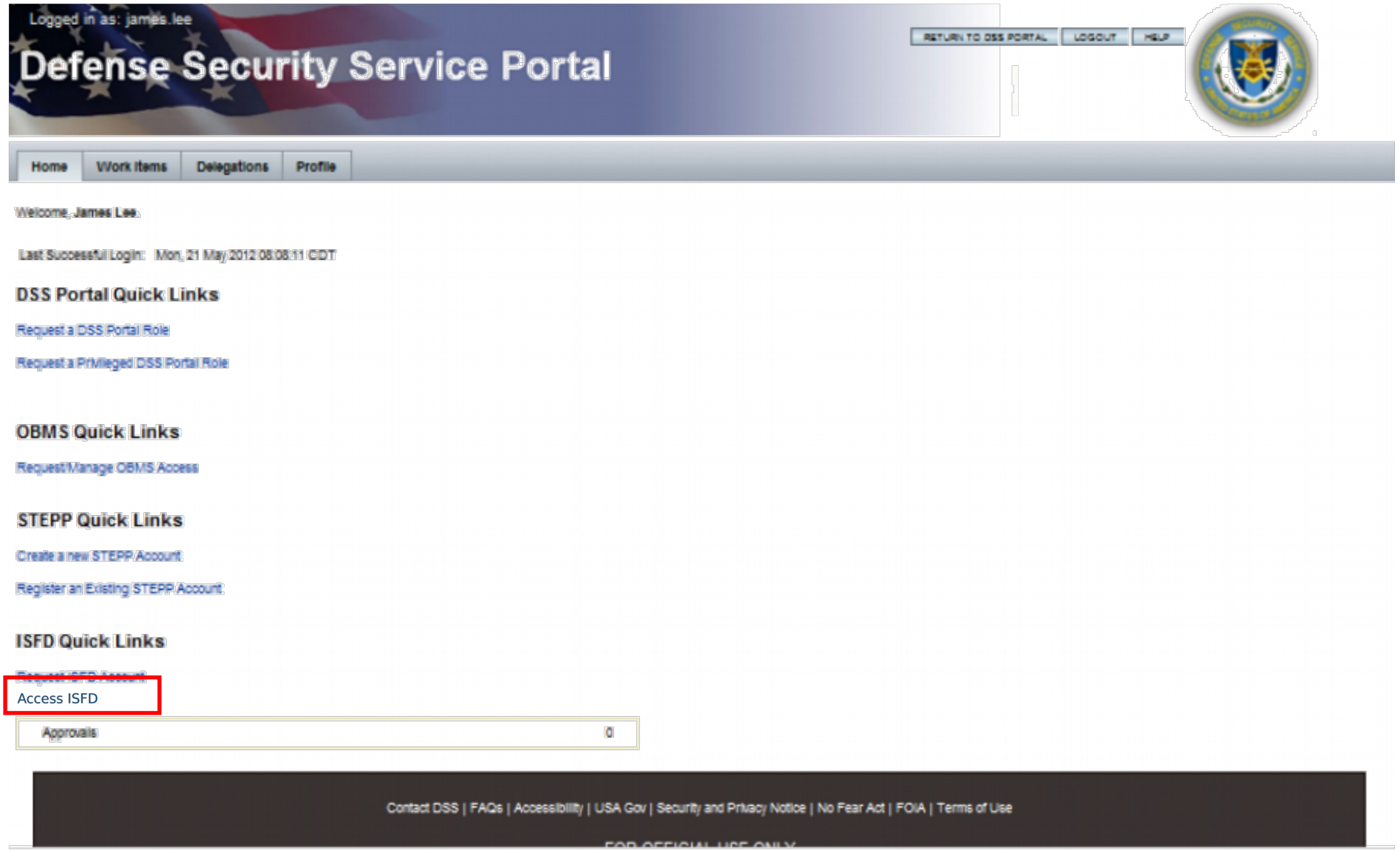
ISFD CAC/PKI Authentication from IdM

Step 1: The User navigates to https://sso.dss.mil.
Step 2: The IdM Solution displays the IdM Portal Disclaimer.
Step 3: The User selects “I Accept” to proceed.
Steps 4-7: Continue as previously referenced.


Welcome | DSS Portal - Windows Internet Explorer
https://sso.dss.mil/opensso/cert/login
Favorites
Welcome | DSS Portal
Page
Safety
Tools
Defense Security Service Portal
DSS Portal Disclaimer
This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized U.S. government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.
I Accept
Click here
FOR OFFICIAL USE ONLY
Copyright © 2011 - Defense Security Service | All Rights Reserved

ISFD CAC/PKI Authentication from IdM

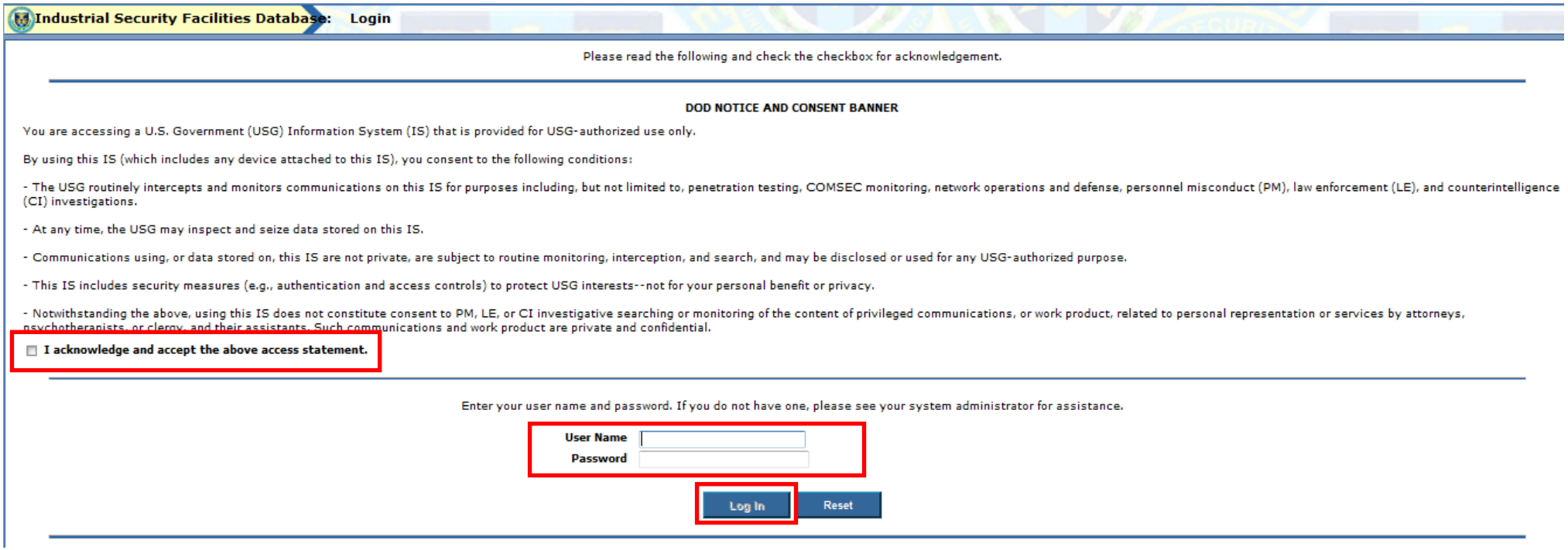
Step 8: The IdM Solution authenticates the User and displays the IdM Portal Home Page.
Step 9: User selects the “Access ISFD” link.


Logged in as: james.lee
Defense Security Service Portal
RETURN TO DSS PORTAL
LOGOUT
HELP
Home
Work Items
Delegations
Profile
Welcome, James Lee.
Last Successful Login: Mon, 21 May 2012 08:08:11 CDT
DSS Portal Quick Links
Request a DSS Portal Role
Request a Privileged DSS Portal Role
OBMS Quick Links
Request/Manage OBMS Access
STEPP Quick Links
Create a new STEPP Account
Register an Existing STEPP Account
ISFD Quick Links
Access ISFD
Approvals
0
Contact DSS | FAQs | Accessibility | USA Gov | Security and Privacy Notice | No Fear Act | FOIA | Terms of Use

ISFD CAC/PKI Authentication from IdM

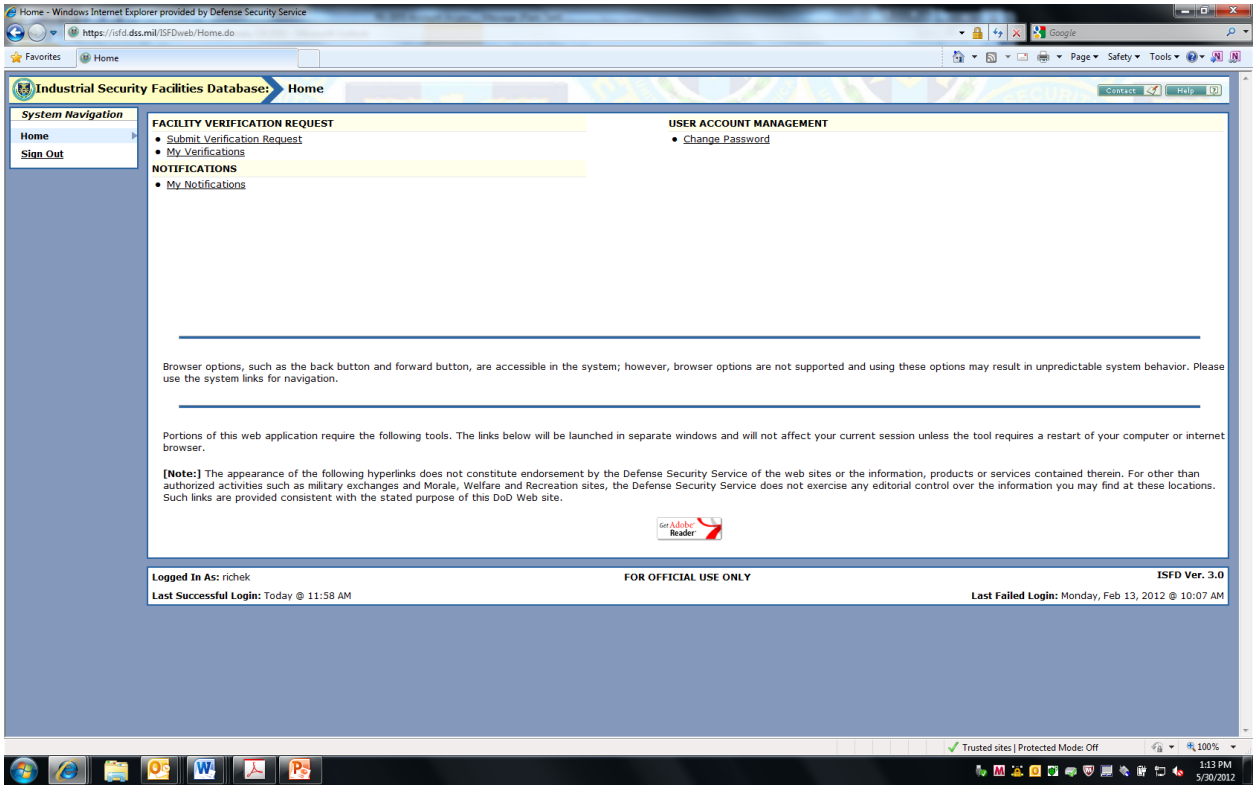
Step 10: The IdM Solution redirects the User to the ISFD Username/Password page.

Step 11: User agrees to the disclaimer, enters his/her ISFD Username and Password, and clicks “Log In”.


Industrial Security Facilities Database: Login
Please read the following and check the checkbox for acknowledgement.
DOD NOTICE AND CONSENT BANNER
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential.
I acknowledge and accept the above access statement.
Enter your user name and password. If you do not have one, please see your system administrator for assistance.
User Name
Password
Log In
Reset

ISFD CAC/PKI Authentication from IdM

Step 12: ISFD authenticates the User and allows full access.


Home - Windows Internet Explorer provided by Defense Security Service
https://isfd.dss.mil/ISFDweb/Home.do
Industrial Security Facilities Database:
Home
System Navigation
Home
Sign Out
FACILITY VERIFICATION REQUEST
Submit Verification Request
My Verifications
NOTIFICATIONS
My Notifications
USER ACCOUNT MANAGEMENT
Change Password
Browser options, such as the back button and forward button, are accessible in the system; however, browser options are not supported and using these options may result in unpredictable system behavior. Please use the system links for navigation.
Portions of this web application require the following tools. The links below will be launched in separate windows and will not affect your current session unless the tool requires a restart of your computer or internet browser.
[Note:] The appearance of the following hyperlinks does not constitute endorsement by the Defense Security Service of the web sites or the information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare and Recreation sites, the Defense Security Service does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this DoD Web site.
Get Adobe Reader
Logged In As: richek
FOR OFFICIAL USE ONLY
ISFD Ver. 3.0
Last Successful Login: Today @ 11:58 AM
Last Failed Login: Monday, Feb 13, 2012 @ 10:07 AM